PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-273259
(43)Date of publication of application : 05.10.2001

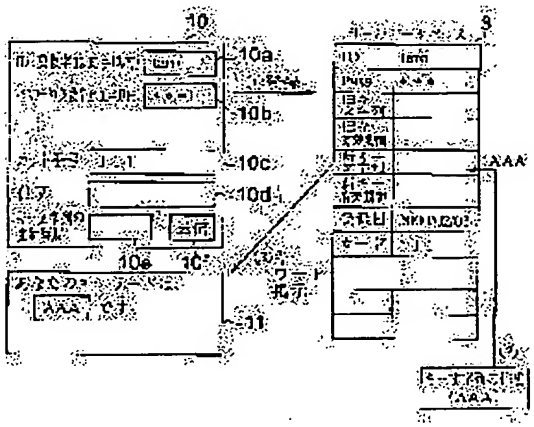
(51)Int.Cl. G06F 15/00
G06F 13/00

(21)Application number : 2000-088947
(22)Date of filing : 28.03.2000

(71)Applicant : MITSUBISHI ELECTRIC SYSTEMWARE CORP
(72)Inventor : ARAKI MICHIKO

(54) SYSTEM AND METHOD FOR USER AUTHENTICATION AND RECORDING MEDIUM RECORDED WITH PROGRAM FOR PERFORMING USER AUTHENTICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To improve security by performing user authentication while using a user ID and a password which are designated by a user and a key character string designated by an authentication system and previously reported to the user.
SOLUTION: When user information required for user registration is inputted to a display picture 10 on a user terminal, a server receivers that information, registers that information in a data base 3, prepares a key character string and displays it on the display picture 11 on the user terminal. The user performs log-in while using the key character string reporting like this together with the user ID and the password. The key character string is periodically changed by the server for improving a security effect.



LEGAL STATUS

[Date of request for examination] 17.09.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－273259
（Ｐ２００１－２７３２５９Ａ）
(43)公開日　平成13年10月５日(2001.10.5)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
G06F 15/00	330	G06F 15/00	330	E 5B085
13/00	354	13/00	354	Z 5B089

審査請求　未請求　請求項の数19　ＯＬ　（全18頁）

(21)出願番号　特願2000－88947(Ｐ2000－88947)

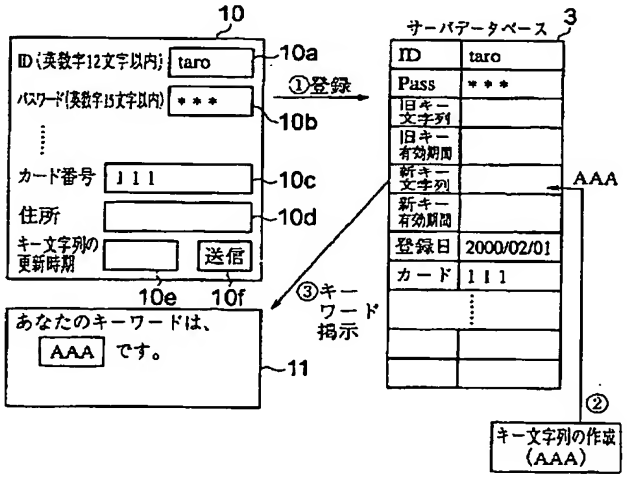
(22)出願日　平成12年３月28日(2000.3.28)

(71)出願人　394013002
三菱電機システムウェア株式会社
神奈川県横浜市戸塚区川上町87番地１
(72)発明者　荒木　美千子
神奈川県横浜市戸塚区川上町87番地１　三菱電機システムウェア株式会社内
(74)代理人　100057874
弁理士　曾我　道照　（外６名）

Ｆターム(参考)　5B085 AA08 AC04 AE02 AE23 BG07
CA04
5B089 GA11 GA21 GB04 HA10 JA31
KA17 KB13 KC58 LB04 LB07
LB14

(54)【発明の名称】ユーザ認証システム、ユーザ認証方法およびユーザ認証を行うためのプログラムを記録した記録媒体

(57)【要約】
【課題】　ユーザにより指定されるユーザＩＤ及びパスワードと認証システムにより指定され、ユーザに事前に通知されているキー文字列とを用いてユーザ認証を行い、安全性を向上させる。
【解決手段】　ユーザ端末の表示画面１０に対してユーザ登録に必要なユーザ情報を入力すると、サーバがそれを受け取り、データベース３内にそれらの情報を登録するとともに、キー文字列を作成して、ユーザ端末の表示画面１１に表示する。ユーザは、このようにして通知されたキー文字列をユーザＩＤ及びパスワードとともに用いてログインを行う。キー文字列は、セキュリティ効果を向上させるため、定期的にサーバにより変更される。



1

【特許請求の範囲】

【請求項１】　登録されるユーザを識別するための固有識別情報を入力するための入力手段と、

上記ユーザを上記固有識別情報に基づいて管理するユーザ管理記憶手段と、

上記ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、上記ユーザ管理記憶手段に登録する認証システム指定特定情報登録手段と、

登録された上記認証システム指定特定情報を上記ユーザに通知する通知手段と、

登録されている上記認証システム指定特定情報を変更もしくは無効にするように上記認証システム指定特定情報登録手段に所定の時間間隔において指示を出力するとともに、上記指示が変更を指示するものであった場合に上記認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力手段と、

上記ユーザからアクセスが行われた場合に、上記ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報を上記ユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、上記ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報を上記ユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合手段と、

上記照合手段による照合のいずれにおいても一致が確認された場合に、上記ユーザに対して使用許可を与える使用許可手段とを備えたことを特徴とするユーザ認証システム。

【請求項２】　上記ユーザを特定するための情報の入力を上記ユーザから受けて、当該情報をユーザ指定特定情報として、上記ユーザ管理記憶手段に登録するユーザ指定特定情報登録手段をさらに備え、

上記照合手段が、上記照合に加えて、さらに、上記ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報を上記ユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定することを特徴とする請求項１記載のユーザ認証システム。

【請求項３】　上記通知手段が、上記認証システム指定特定情報を上記ユーザからの上記固有識別情報の入力があった画面上に表示することにより、上記ユーザに通知することを特徴とする請求項１または２に記載のユーザ認証システム。

【請求項４】　上記通知手段が、上記認証システム指定特定情報を電子メールにより上記ユーザに通知することを特徴とする請求項１または２に記載のユーザ認証システム。

【請求項５】　上記通知手段が、上記認証システム指定特定情報をＦＡＸにより上記ユーザに通知することを特

2

徴とする請求項１または２に記載のユーザ認証システム。

【請求項６】　上記通知手段が、上記認証システム指定特定情報を所定の郵便物により上記ユーザに通知することを特徴とする請求項１または２に記載のユーザ認証システム。

【請求項７】　上記通知手段が、上記認証システム指定特定情報を暗号化して上記ユーザに送信することを特徴とする請求項１～４のいずれかに記載のユーザ認証システム。

【請求項８】　課金・請求処理を行うための課金処理手段をさらに備えたことを特徴とする請求項１～７のいずれかに記載のユーザ認証システム。

【請求項９】　上記認証システム指定特定情報の上記有効期間に対して課金・請求処理を行うための課金処理手段をさらに備えたことを特徴とする請求項１～７のいずれかに記載のユーザ認証システム。

【請求項１０】　登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、

上記ユーザを上記固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、

上記ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、上記データベースに登録する認証システム指定特定情報登録ステップと、

登録された上記認証システム指定特定情報を上記ユーザに通知する通知ステップと、

登録されている上記認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、上記指示が変更を指示するものであった場合に上記認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、

上記指示に基づいて、上記データベースに登録されている上記認証システム指定特定情報を変更または無効にして上記データベースに再登録する認証システム指定特定情報再登録ステップと、

上記ユーザからアクセスが行われた場合に、上記ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報を上記ユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、上記ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報を上記ユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、

上記照合手段による照合のいずれにおいても一致が確認された場合に、上記ユーザに対して使用許可を与える使用許可ステップとを備えたことを特徴とするユーザ認証方法。

【請求項１１】　上記ユーザを特定するための情報の入力を上記ユーザから受けて、当該情報をユーザ指定特定

情報として、上記データベースに登録するユーザ指定特定情報登録手段をさらに備え、
上記照合ステップにおいて、上記照合に加えて、さらに、上記ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報を上記ユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定することを特徴とする請求項１０記載のユーザ認証方法。

【請求項１２】　上記通知ステップにおいて、上記認証システム指定特定情報を上記ユーザからの上記固有識別情報の入力があった画面上に表示することにより上記ユーザに通知することを特徴とする請求項１０または１１に記載のユーザ認証方法。

【請求項１３】　上記通知ステップにおいて、上記認証システム指定特定情報を電子メールにより上記ユーザに通知することを特徴とする請求項１０または１１に記載のユーザ認証方法。

【請求項１４】　上記通知ステップにおいて、上記認証システム指定特定情報をＦＡＸにより上記ユーザに通知することを特徴とする請求項１０または１１に記載のユーザ認証方法。

【請求項１５】　上記通知ステップにおいて、上記認証システム指定特定情報を所定の郵便物により上記ユーザに通知することを特徴とする請求項１０または１１に記載のユーザ認証方法。

【請求項１６】　上記通知ステップにおいて、上記認証システム指定特定情報を暗号化して上記ユーザに送信することを特徴とする請求項１０～１３のいずれかに記載のユーザ認証方法。

【請求項１７】　課金・請求処理を行うための課金処理ステップをさらに備えたことを特徴とする請求項１０～１６のいずれかに記載のユーザ認証方法。

【請求項１８】　上記認証システム指定特定情報の上記有効期間に対して課金・請求処理を行うための課金処理ステップをさらに備えたことを特徴とする請求項１０～１６のいずれかに記載のユーザ認証方法。

【請求項１９】　ユーザ認証を行うためのプログラムを記録した記録媒体であって、
登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、
上記ユーザを上記固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、
上記ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、上記データベースに登録する認証システム指定特定情報登録ステップと、
登録された上記認証システム指定特定情報を上記ユーザに通知する通知ステップと、
登録されている上記認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、上記指示が変更を指示するものであった場合に上記認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、
上記指示に基づいて、上記データベースに登録されている上記認証システム指定特定情報を変更または無効にして上記データベースに再登録する認証システム指定特定情報再登録ステップと、
上記ユーザからアクセスが行われた場合に、上記ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報を上記ユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、上記ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報を上記ユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、
上記照合手段による照合のいずれにおいても一致が確認された場合に、上記ユーザに対して使用許可を与える使用許可ステップとを備えたことを特徴とするプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はユーザ認証システム及びユーザ認証方法に関し、特に、パーソナルコンピュータやワークステーション、及び、インターネットに接続されたサーバ等の種々の情報処理装置において、ユーザを特定する特定情報が入力された場合に、その特定情報の入力がユーザ本人によって行われたか否かを認証して、不正アクセスを防止するためのユーザ認証システム、ユーザ認証方法およびユーザ認証を行うためのプログラムを記録した記録媒体に関するものである。

【０００２】

【従来の技術】従来の一般的なこの種のユーザ認証方法としては、ホストコンピュータやサーバ等の認証システム上に前もって個々のユーザのＩＤ番号毎にパスワードを登録しておき、使用開始時にユーザＩＤとパスワードとをキーボード等の入力装置から入力させて、前もって登録しておいた正規のユーザＩＤ及びパスワードとの照合を行い、一致した場合に使用許可を与えるという方法が多く用いられている。

【０００３】図１９は、このような従来のユーザ認証システムが接続されたネットワークシステムの構成を示した図である。図１９は、インターネットに代表されるネットワークシステムを例に挙げており、図において、１００は任意のWWW（WorldWide Web）ブラウザと任意の電子メール送受信用ソフトウエアを使用するユーザ端末、１０１はインターネット等のネットワーク、１０２ａ，１０２ｂ，１０２ｃは、ネットワーク１０１に接続され、個々のホームページを開設している複数のサーバ、１０３ａ，１０３ｂ，１０３ｃは、各サーバ１０２ａ，１０２ｂ，１０２ｃに接続されているデータベース

で、ユーザＩＤ毎にパスワードが予め格納されている。

【０００４】動作について説明する。ユーザ端末１００の利用者であるユーザが、例えば、任意のWWWブラウザを用いて、ネットワーク１０１を介して、サーバ１０２ａが開設するホームページの会員となり、ユーザＩＤの発行を受け、所定のパスワードの登録をすでに行っているものとする。このとき、ユーザが、ネットワーク１０１を介して、サーバ１０２ａのホームページにアクセスすると、サーバ１０２ａは、ユーザに対して、ユーザＩＤとパスワードの入力を要求する。この要求に対して、ユーザがユーザＩＤとパスワードを入力すると、データベース１０３ａ内に前もって登録されている正規のユーザＩＤ及びパスワードとユーザにより今回入力されたユーザＩＤ及びパスワードとの照合が行われ、これらが一致した場合にユーザは使用許可を得ることができ、サーバ１０２ａはネットワーク１０１を介してホームページにおける種々のデータをユーザ端末１００に送信し、それらを表示させる。

【０００５】

【発明が解決しようとする課題】従来のユーザ認証方法においては、上述したように、ユーザＩＤとパスワードのみでの認証であり、パスワードが第三者に漏れる可能性を考慮して、ユーザが頻繁にパスワードを変更すれば安全性が高まるが、頻繁に変更するためにはユーザの手間がかかるとともに、あまりに頻繁に変更するとユーザの記憶が混乱しパスワードがわからなくなってしまう等の問題が起き、ユーザに要求される負担が大きいため、パスワードを滅多に変更しないユーザがほとんどであるのが現状である。

【０００６】この発明は、かかる問題点を解決するためになされたものであり、認証システム側により定期的に変更されてユーザに通知される所定の文字列を用いてユーザ認証を行うことにより、安全性を高め、第三者による不正アクセスを防止するユーザ認証システム、ユーザ認証方法およびユーザ認証を行うためのプログラムを記録した記録媒体を得ることを目的とする。

【０００７】

【課題を解決するための手段】この発明は、登録されるユーザを識別するための固有識別情報を入力するための入力手段と、ユーザを固有識別情報に基づいて管理するユーザ管理記憶手段と、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、ユーザ管理記憶手段に登録する認証システム指定特定情報登録手段と、登録された認証システム指定特定情報をユーザに通知する通知手段と、登録されている認証システム指定特定情報を変更もしくは無効にするように認証システム指定特定情報登録手段に所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力手段と、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合手段と、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可手段とを備えたユーザ認証システムである。

【０００８】また、ユーザを特定するための情報の入力をユーザから受けて、当該情報をユーザ指定特定情報として、ユーザ管理記憶手段に登録するユーザ指定特定情報登録手段をさらに備え、照合手段が、上記照合に加えて、さらに、ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報をユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定する。

【０００９】また、通知手段が、認証システム指定特定情報を、ユーザからの固有識別情報の入力があった画面上に表示することによりユーザに通知する。

【００１０】また、通知手段が、認証システム指定特定情報を電子メールによりユーザに通知する。

【００１１】また、通知手段が、認証システム指定特定情報をＦＡＸによりユーザに通知する。

【００１２】また、通知手段が、認証システム指定特定情報を所定の郵便物によりユーザに通知する。

【００１３】また、通知手段が、認証システム指定特定情報を暗号化してユーザに送信する。

【００１４】また、課金・請求処理を行うための課金処理手段をさらに備えている。

【００１５】また、認証システム指定特定情報の有効期間に対して課金・請求処理を行うための課金処理手段をさらに備えている。

【００１６】また、この発明は、登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、ユーザを固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、データベースに登録する認証システム指定特定情報登録ステップと、登録された認証システム指定特定情報をユーザに通知する通知ステップと、登録されている認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、指示に基づいて、データベースに登録されている認証システム指定特定情報を変更または無効にしてデータベースに再登録する認証システム

指定特定情報再登録ステップと、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可ステップとを備えたユーザ認証方法である。

【００１７】また、ユーザを特定するための情報の入力をユーザから受けて、当該情報をユーザ指定特定情報として、データベースに登録するユーザ指定特定情報登録手段をさらに備え、照合ステップにおいて、上記照合に加えて、さらに、ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報をユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定する。

【００１８】また、通知ステップにおいて、認証システム指定特定情報を、ユーザからの固有識別情報の入力があった画面上に表示することによりユーザに通知する。

【００１９】また、通知ステップにおいて、認証システム指定特定情報を電子メールによりユーザに通知する。

【００２０】また、通知ステップにおいて、認証システム指定特定情報をＦＡＸによりユーザに通知する。

【００２１】また、通知ステップにおいて、認証システム指定特定情報を所定の郵便物によりユーザに通知する。

【００２２】また、通知ステップにおいて、認証システム指定特定情報を暗号化してユーザに送信する。

【００２３】また、課金・請求処理を行うための課金処理ステップをさらに備えている。

【００２４】また、認証システム指定特定情報の有効期間に対して課金・請求処理を行うための課金処理ステップをさらに備えている。

【００２５】また、この発明は、ユーザ認証を行うためのプログラムを記録した記録媒体であって、登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、ユーザを固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、データベースに登録する認証システム指定特定情報登録ステップと、登録された認証システム指定特定情報をユーザに通知する通知ステップと、登録されている認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、指示に基づいて、データベースに登録されている認証システム指定特定情報を変更または無効にしてデータベースに再登録する認証システム指定特定情報再登録ステップと、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可ステップとを備えたプログラムを記録した記録媒体である。

【００２６】

【発明の実施の形態】実施の形態１．図１は、本発明におけるユーザ認証システムの構成を示した概略構成図である。図１において、１は任意のWWWブラウザと任意の電子メール送受信用ソフトウエアとを使用するユーザ端末、２は、インターネット等のネットワーク１０１に接続され、登録制のホームページを開設しているサーバであり、３は、サーバ２に接続され、登録されたユーザをユーザＩＤ（固有識別情報）に基づいて管理記憶するデータベースで、ユーザＩＤ毎にパスワードと後述するキー文字列とを含むユーザ情報を格納している。なお、本実施の形態においては、サーバ２とデータベース３とがユーザ認証システムを構成している。

【００２７】次に、サーバ２の内部構成について説明する。２ａは、ユーザ端末１との間のデータの入出力を制御するユーザインターフェース手段、２ｂは、ユーザを特定するためのパスワードの入力をユーザから受けて、当該パスワードをユーザ指定特定情報として、データベース３に登録するユーザ指定特定情報登録手段、２ｃは、ユーザを特定するためのキー文字列を発行し、当該キー文字列を認証システム指定特定情報として、データベース３に登録する認証システム指定特定情報登録手段、２ｄは、登録されたキー文字列をユーザに通知する通知手段、２ｅは、登録されているキー文字列を変更もしくは無効にするための再登録を行うように認証システム指定特定情報登録手段２ｃに所定の時間間隔において指示を出力する変更／無効指示出力手段である。また、２ｆは、ユーザからアクセスが行われた場合に、ユーザからユーザＩＤの入力を受け付けて、入力されたユーザＩＤをデータベースに登録されているユーザＩＤと照合し、一致するか否かを判定する第一の照合手段、２ｇは、第一の照合手段２ｆにより一致が確認された場合に、ユーザからパスワードの入力を受け付けて、入力されたパスワードをデータベース３に登録されているパスワードと照合し、一致するか否かを判定する第二の照合

手段、２ｈは、第二の照合手段２ｇにより一致が確認された場合に、ユーザからキー文字列の入力を受け付けて、入力されたキー文字列をデータベース３に登録されているキー文字列と照合し、一致するか否かを判定する第三の照合手段である。また、２ｊはホームページ等の動作のためのメインプログラムが格納されているメインプログラム格納手段で、２ｉは、当該メインプログラムによりサーバ２の内部動作の制御を行う制御手段であり、上述の第三の照合手段２ｈにより一致が確認された場合に、ユーザに対して使用許可を与える動作も行うものである。また、２ｋは、データベース３との間のデータの入出力を制御するデータベースインターフェース手段である。

【００２８】動作について説明する。図２は、サーバ２のホームページにユーザ登録を行うための処理の流れを示したフローチャートであり、図３は、その動作を説明するための説明図である。図３において、１０はユーザ登録を行うためのユーザ端末１における表示画面、１１はユーザ登録後のユーザ端末１の表示画面である。表示画面１０には、図のように、ユーザＩＤ、パスワード、カード番号、住所等のユーザ情報の入力を行うための入力欄１０ａ～１０ｄが設けられている。また、図３に、サーバ２に接続されているデータベース３の一例が示されており、データベース３には、図のように、ユーザＩＤ、パスワード、旧キー文字列、旧キー文字列の有効期間、新キー文字列、新キー文字列の有効期間、登録日、カード番号等が格納されている。

【００２９】図２のフローチャートに示すように、まず、ステップＳ１において、サーバ２が開設するホームページにユーザ登録を行いたいユーザは、任意のＷＷＷブラウザを用いて、ネットワーク１０１を介して、当該ホームページにアクセスし、ユーザ端末１に設けられたキーボード及びマウス等の入力手段（図示せず）により、表示画面１０の入力欄１０ａ～１０ｄに対して、ユーザＩＤ、パスワード、カード番号、住所等の項目について入力を行う。入力が終わると、ユーザは、表示画面１０の「送信」ボタン１０ｆをクリックして、データをサーバ２に送信する指示をユーザ端末１に与える。当該指示により、入力されたデータは、ネットワーク１０１を介して、サーバ２に送信され、サーバ２は、ユーザインターフェース手段２ａにより当該データを受信すると、制御手段２ｉにより、ステップＳ２において、必要な項目がすべて入力されているか否かを判定し、入力されていた場合には、ステップＳ３において、入力されたデータが不正な値か否かを判定し、不正でない場合には、ステップＳ４において、認証システム指定特定情報登録手段２ｃによりキー文字列の作成を行う。ここで、キー文字列とは、サーバ２が所定の時間間隔で変更させる文字列で、例えば、数字、アルファベットまたは記号からなる文字列、もしくは、それらの組合せから構成されるものであり、ユーザＩＤ及びパスワードとともに、ユーザ認証に用いる特定情報の１つである。作成方法としては、乱数等を用いてランダムに発生させてもよく、また、サーバ側のオペレータ等が適当に定めた所定の文字列から構成するようにしてもよい。文字列の長さとしては、４ケタ～８ケタ程度が、実用上かつ安全性上適当である。次に、ステップＳ５において、認証システム指定特定情報登録手段２ｃが、ステップＳ４で作成したキー文字列（図３の例では“ＡＡＡ”とする）、ユーザＩＤ、パスワード等をデータベース３に登録する。次に、通知手段２ｄにより、ステップＳ６において、ユーザ端末１にネットワーク１０１を介して当該キー文字列を送信し、図３に示すように、ユーザ端末１の表示画面１１に、例えば、「あなたのキーワードはＡＡＡです。」のようにキー文字列を表示してユーザに掲示する。以上でユーザ登録は完了するので、ステップＳ７の所望のメイン処理に移行する。なお、上述のステップＳ２またはＳ３において、ユーザによって入力されたデータが適切でないと判定された場合には、ステップＳ８において、登録不成功のメッセージがユーザ端末１の表示画面に表示される。

【００３０】ここで、キー文字列は、上述したように、サーバ２により所定の時間間隔で変更されるものであり、従って、所定の期限内で有効であり、期限が経過すると、その時点で無効となる。この期限は原則としてサーバ側で予め定めた所定の期間とするが、複数の期限の候補を用意しておき、すなわち、１ケ月、２ケ月、３ケ月というように用意しておいて、それをユーザが選択できるようにしてもよい。また、ユーザ側がキー文字列の更新時期を指定できるようにしてもよい。ユーザが選択または指定する場合には、上述の図３の表示画面１０の入力欄１０ｅを用いて、キー文字列の更新時期を入力するようにすればよい。

【００３１】図４は、キー文字列の有効期限内にユーザがログインする場合の処理の流れを示したフローチャートである。また、図５は、その動作を説明するための説明図である。図５において、１２はログインを行うためのユーザ端末１における表示画面、１３はログイン後のユーザ端末１の表示画面である。

【００３２】図４に示すように、まず、ステップＳ１１において、ログインを行いたいユーザは、ユーザ端末１に設けられたキーボード及びマウス等の入力手段（図示せず）を用いて、表示画面１２の入力欄１０ｇに対して、ユーザＩＤの入力を行う。入力されたユーザＩＤは、ネットワーク１０１を介して、サーバ２に送信される。サーバ２は、当該データを受信すると、ステップＳ１２において、第一の照合手段２ｆにより、データベース３内のデータを検索して、入力されたユーザＩＤが登録されているか否かを判定し、入力されていた場合には、ステップＳ１３において、入力されたユーザＩＤが

使用可能のものか否かを判定する。使用可能であった場合には、ステップＳ１４において、表示画面１２の入力欄１０ｈにパスワードの入力を行うようにユーザに促す。ユーザがそれに従い、パスワードを入力すると、サーバ２がそれを受信する。次に、ステップＳ１５において、第二の照合手段２ｇにより、入力されたパスワードとデータベース３内に予め登録されている正規のパスワードとの照合を行い、パスワードが一致していた場合には、次に、ステップＳ１６において、表示画面１２の入力欄１０ｉにキー文字列の入力を行うようにユーザに促す。ユーザがそれに従い、キー文字列を入力すると、サーバ２がそれを受信し、次に、ステップＳ１７において、第三の照合手段２ｈにより、入力されたキー文字列とデータベース３内に予め登録されている正規のキー文字列との照合を行い、キー文字列が一致していた場合には、ユーザに使用許可が与えられ、図５の表示画面１３に示されるように、ログイン成功のメッセージが表示される。以上でログイン処理が完了されるので、ステップＳ１８のメイン処理に移行される。なお、上述のステップＳ１２、Ｓ１３、Ｓ１５またはＳ１７において、ユーザによって入力されたユーザＩＤ、パスワード、または、キー文字列が適切でないと判定された場合には、ステップＳ１９において、ログイン不成功のメッセージがユーザ端末１の表示画面に表示される。

【００３３】次に、キー文字列の有効期限が経過した場合の更新の処理について説明する。前提条件として、本実施の形態においては、キー文字列の有効期限は、ユーザ登録の日付にかかわらず、毎月の１日～末日までとする。現時点においては、先のキー文字列の有効期限はすでに経過しており、サーバ２の変更／無効指示出力手段２ｅにより認証システム指定特定情報登録手段２ｃに指示が出され、先のキー文字列は無効となっているものとする。なお、認証システム指定特定情報登録手段２ｃのキー文字列を無効にする動作としては、データベース３内の新キー文字列のデータ領域に格納されているキー文字列をデータベース３内の旧キー文字列のデータ領域に移動させるとともに、新しいキー文字列として、例えば“ＮＵＬＬ”を発行し、それをデータベース３内の新キー文字列のデータ領域に登録するようにすればよい。

【００３４】図６は、旧キー文字列が無効となった以降に最初にユーザがログインする場合のキー文字列の更新の処理の流れを示したフローチャートであり、図７は、その動作を説明するための説明図である。図６に示すように、まず、ステップＳ２１において、ログインしたいユーザは、ユーザ端末１に設けられたキーボード及びマウス等の入力手段（図示せず）を用いて、図７の表示画面１２の入力欄１０ｇ～１０ｉに対して、ユーザＩＤ、パスワード、キー文字列の入力を行う（この場合のキー文字列は、無効となっている旧キー文字列である。）。入力されたこれらのデータは、ネットワークを介して、

サーバ２に送信される。サーバ２は、当該データを受信すると、ステップＳ２２において、データベース３内のデータを検索して、キー文字列の有効期限を確認し、有効期限が経過していた場合には、データベース３内の旧キー文字列に当該データが登録されているか否かを判定し、登録されていた場合には、ステップＳ２３において、図７の表示画面１４の入力欄１０ｊ（Yes）及び１０ｋ（No）に対して、契約を更新するか否かの希望を入力するようにユーザに促す。ユーザがそれに従い、“更新（Yes）”を選択すると、サーバ２がそれを受信し、次に、ステップＳ２４において、キー文字列の作成を行う。キー文字列の作成方法等については、上述と同様であるため、ここでは説明を省略する。次に、ステップＳ２５において、ステップＳ２４で新規に作成したキー文字列（図７の例では“ＺＺＺ”とする）をデータベース３内の新キー文字列のデータ領域に登録する。次に、ステップＳ２６において、ユーザ端末１にネットワークを介して当該キー文字列を送信し、図７に示すように、ユーザ端末１の表示画面１５に、例えば、「あなたの今月のキーワードはＺＺＺです。」のようにキー文字列を表示してユーザに掲示する。以上でキー文字列の更新処理は完了するので、ステップＳ２７の所望のメイン処理に移行する。なお、上述のステップＳ２２において、ユーザによって入力されたユーザＩＤ等が登録されていないと判定された場合、及び、ステップＳ２３において、ユーザが“契約を更新せず（No）”を選択した場合には、ステップＳ２８において、更新不成功のメッセージがユーザ端末１の表示画面に表示される。

【００３５】以上のように、本実施の形態においては、ユーザ側により登録されるユーザＩＤ及びパスワードに加え、サーバ側により定期的に変更されてユーザに通知される所定のキー文字列を用いて、これら３種類の情報を組み合わせてユーザ認証を行うようにしたので、安全性が向上する。また、たとえ、ユーザがパスワードを頻繁に変更する作業を怠っていても、サーバ側によりキー文字列は強制的に変更されるので、第三者にユーザＩＤ、パスワード、キー文字列のすべてが万一漏れた場合にも、次のキー文字列が発行された時点で、これらの漏れた特定情報は無効になるため、第三者の不正アクセスを最小限に食い止めることができる。

【００３６】なお、上述の例では、キー文字列の有効期限をユーザ登録の日付にかかわらず、毎月の１日～末日までとする例について述べたが、その場合に限らず、本発明はキー文字列をサーバ２が強制的に変更することを目的としているため、例えば、ユーザ登録の日から１ケ月というように、有効期限の起算日をユーザ登録した日としてもよく、また、１ケ月ではなく、毎日ないし１週間程度で変更するようにしてもよい。

【００３７】また、上述の例では、ユーザからの契約更新の指示を受けて、新しいキー文字列を発行する例につ

いて述べたが、その場合に限らず、有効期限が経過したら、自動的に、変更／無効指示出力手段２ｅの指示により、新しいキー文字列が発行されて、それがデータベース３に登録されるとともに、ユーザに通知されるようにしてもよい。

【００３８】実施の形態２．上述の実施の形態１においては、サーバ２により作成されたキー文字列をＷＷＷブラウザによりユーザに対して掲示する方法について述べたが、本実施の形態においては、電子メールによりユーザに対して通知する例について説明する。図８は本実施の形態におけるユーザ登録動作の処理の流れを説明するための説明図であり、図９はキー文字列の期限経過後の更新動作の処理の流れを説明するための説明図である。これらの図において、４は、サーバ２に接続され、メールの送受信を行うメールサーバであり、図８の１０ｍ及び１０ｎはメールアドレス及びユーザが契約しているプロバイダ名を入力するための入力欄であり、図８の４０及び図９の４１は共にメールサーバ４によりユーザに対して配信された電子メールである。他の構成については上述の実施の形態１と同一であるため、同一符号を付して示している。なお、本実施の形態における有効期限内のログイン動作については、上述の実施の形態１（図４及び図５参照）と同一であるため、ここでは説明を省略する。

【００３９】動作について説明する。まずはじめに、ユーザ登録動作について説明する。処理の流れは、基本的には図２のフローチャートと同様であるため、これを参照しながら説明する。まず、ステップＳ１において、上述の実施の形態１で示したユーザＩＤ等の項目に加えて、本実施の形態においては、メールアドレス及びユーザが契約しているプロバイダ名を入力する。ステップＳ２～Ｓ５までの処理は全く同一である。ステップＳ６において、本実施の形態では、ユーザ登録を行ったユーザに対して、契約してある所定のプロバイダを介して、電子メールを配信し、図８に示すように、例えば、「あなたのキーワードはＡＡＡです。」のようにキー文字列を通知する。本実施の形態においては、以上でユーザ登録は完了する（ここでは、図２のステップＳ７のメイン処理の工程はない。）。なお、図２のステップＳ２またはＳ３において、ユーザによって入力されたデータが適切でないと判定された場合には、ステップＳ８において、登録不成功のメッセージをユーザ端末１の表示画面に表示させる。

【００４０】次に、キー文字列の期限満了後の更新動作について説明する。この処理は、基本的に図６のフローチャートと同様であるため、これを参照しながら説明する。ステップＳ２１～Ｓ２５までの処理は全く同一である。ステップＳ２６において、本実施の形態においては、契約を更新したユーザに対して、契約してある所定のプロバイダを介して、電子メールを配信し、図９に示すように、例えば、「あなたの今月のキーワードはＺＺＺです。」のようにキー文字列を通知する。本実施の形態においては、以上でキー文字列の更新処理は完了する（ここでは、ステップＳ２７のメイン処理の工程はない。）。なお、図６のステップＳ２２において、ユーザによって入力されたユーザＩＤ等が登録されていないと判定された場合、及び、ステップＳ２３において、ユーザが“契約を更新せず（No）”をユーザが選択した場合には、ステップＳ２８において、更新不成功のメッセージをユーザ端末１の表示画面に表示させる。

【００４１】以上のように、本実施の形態においては、上述の実施の形態１と同様の効果が得られるとともに、さらに、サーバ２が作成したキー文字列を電子メールを介してユーザに通知するようにしたので、ユーザ端末１からサーバ２にアクセスする経路（ネットワーク）とは別の経路（電子メール）でユーザに通知するようにしたので、キー文字列を第三者に盗み取られる危険性をより低減できる効果がある。

【００４２】なお、本実施の形態においては、キー文字列をユーザに通知するための媒体として電子メールを用いる例につて述べたが、その場合に限らず、例えば、ＦＡＸや郵便物により通知するようにしても、同様の効果が得られる。本明細書においては、郵便物として、郵便によるハガキ、手紙等の郵便物全般、電報、及び、宅急便等による配達物をすべて含むものとする。

【００４３】実施の形態３．上述の実施の形態１においては、サーバが作成したキー文字列をネットワークを介して送信し、また、ユーザがログインする時などに、ユーザ端末１からサーバ２へユーザＩＤ、パスワード、キー文字列を送信するが、このとき、いずれもネットワークを介して送信するため、第三者にそれらの情報を盗み取られる危険性がある。そのため、本実施の形態においては、これらの情報を送信する際に暗号化して送信する例について説明する。暗号化アルゴリズムは、大きく分けて、共通鍵暗号方式と公開鍵暗号方式の２種類の方式がある。

【００４４】共通鍵暗号方式の場合について簡単に説明すれば、この方式においては暗号化する鍵と復号化する鍵が同じ鍵であるので、ユーザ端末１とサーバ２とがお互いに共通鍵を保持しておき、送信する場合に情報をその共通鍵で暗号化して送信し、相手方がそれを受信したら、自分が保持している共通鍵で復号化する。

【００４５】また、公開鍵暗号方式について簡単に説明すれば、その代表的なものにＲＳＡ方式があり、暗号化鍵と復号化鍵が異なる方式であるため、２種類の鍵を作成する必要がある。一方が送り手が保持する鍵で秘密鍵と呼ばれるものであり、他方が相手方に渡しておく鍵で公開鍵と呼ばれるものである。ユーザ端末１及びサーバ２はお互いに相手の公開鍵を保持しているとする。従って、ユーザ端末１は自分の秘密鍵Ａとサーバ２の公開鍵

Ｂとを保持し、サーバ２は自分の秘密鍵Ｂとユーザ端末１の公開鍵Ａとを保持している。ユーザ端末１は秘密鍵Ａで暗号化して送ることも、公開鍵Ｂで暗号化して送ることもできる。公開鍵Ｂで暗号化して送ればサーバ２が有する秘密鍵Ｂでしか解読できないので、第三者に対する安全性を確保することができる。また、秘密鍵Ａで暗号化して送れば、安全性の確保に加えて、秘密鍵Ａを保持しているのはユーザ端末１のみであるので、情報の送り手がユーザ端末１であるという認証を同時に行えることができる。サーバ２についても同様である。

【００４６】以上のように、本実施の形態においては、上述の実施の形態１の効果に加えて、さらに、ユーザ端末１とサーバ２との間で、パスワードやキー文字列のように第三者に知られたくない情報を暗号化して送るようにしたので、より安全性を確保することができる。

【００４７】実施の形態４．本実施の形態においては、上述の実施の形態１～３の構成に、さらに、課金処理手段を追加した例について説明する。図１０は、図３の例に課金処理手段を追加した例を示している。図１０において、３０は、サーバ２に接続されたデータベース３内に追加された課金情報データ、５はサーバ２内に設けられ、課金・請求処理を行う課金処理手段である。課金情報データ３０としては、図のように、請求期間、使用料金、使用料金の請求先、引き落とし口座等の情報が格納されている。

【００４８】動作について説明する。ユーザ登録の処理の流れは、基本的には図２のフローチャートと同様であるため、これを参照しながら説明する。まず、ステップＳ１において、上述の実施の形態１で示したユーザＩＤ等の項目に加えて、本実施の形態においては、課金処理に必要な使用料金請求先と引き落とし口座を入力する。ステップＳ２～Ｓ４までの処理は全く同一である。ステップＳ５において、データベースへデータを登録する際に、本実施の形態においては、課金処理に必要な情報をデータベース３に格納する処理が追加される。ただし、使用料金の項目の初期値は“０”に自動設定されるものとする。以降のステップＳ６～Ｓ８の処理は図２と同じであるため説明は省略するが、ステップＳ７のメイン処理において、その都度、使用量に応じて使用料金が課金され、課金テーブル３０の使用料金の値にその値が加算される。

【００４９】有効期限内のログイン動作及びキー文字列の更新動作については実施の形態１と基本的に同じであるが、それぞれ、メイン処理において、その使用量に応じて使用料金が課金され、上述と同様に加算される。

【００５０】課金処理手段５は、常に課金テーブル３０内の有効期限をチェックし、有効期限が経過したら、有効期限日までの使用料金の合計値を課金テーブル３０から読み出して、口座からの引き落とし処理を行うようにユーザより指定された銀行に通知するか、または、ユーザの住所宛に郵送するための請求書を作成する。

【００５１】以上のように、本実施の形態においては、課金処理手段５を追加したので、上述の実施の形態１～３の効果に加えて、さらに、ユーザに対して使用料金を自動的に請求することができるので、利便性が向上する。

【００５２】実施の形態５．上述の実施の形態１～４については、キー文字列を単にユーザ認証の安全性を高めるために用いる例について述べたが、以下の実施の形態においては、キー文字列のユーザ認証目的に加えた付加的な使用目的について説明する。本実施の形態においては、月単位でプロバイダとの契約を結ぶためにキー文字列を用いる例について説明する。図１１はユーザ登録、図１２は契約期間内でのログイン、図１３は契約更新の動作を説明するための説明図である。

【００５３】動作について説明する。図１１に示すように、ユーザ登録を行う際に、ユーザＩＤとパスワード等を入力して、「契約」ボタン１６ａを押すと、サーバ２から１ケ月間（例えば２０００年１月１日～２０００年１月３１日）だけ有効なキー文字列が提供される。１月３１日まではそのキー文字列を使って、図１２に示すようにログインできるが、２月１日からはログインできないようにする。

【００５４】２月１日以降にログインしようとすると、サーバ２がキー文字列から有効期限が切れていることを検出し、図１３の表示画面１７に示すように、「キー文字列の期限が切れています。契約を更新しますか？」というメッセージを表示する。ユーザがそれに対して、契約更新（Yes）するか否か（No）を選択する。契約更新を選択した場合には、サーバ２により、新しいキー文字列が作成され、ユーザに対して通知される。

【００５５】以上のように、本実施の形態においては、ユーザＩＤ、パスワード、キー文字列の３つによりユーザの認証を行って、ユーザに使用許可を与えるようにしたので、安全性が高く、契約していない第三者により不正にアクセスされることが防止できるとともに、さらに、月単位のように所定の日数の単位でキー文字列を変更することにより、所定の日数の単位での契約を人手を介さずに自動的に更新することができるので、プロバイダ側での契約更新の作業効率を向上させることができる。

【００５６】実施の形態６．本実施の形態においては、キー文字列の有効期間に対して課金・請求処理を行う例について説明する。なお、ユーザ登録、キー文字列の有効期間内でのログイン及びキー文字列の更新の動作については、上述の実施の形態１と同じであるため説明を省略する。

【００５７】動作について説明する。実施の形態１で述べたように、ユーザ登録を行うと、サーバ２から、所定の有効期間において有効なキー文字列が発行される。本

実施の形態においては、このキー文字列の有効期間に対して課金・請求処理を行う、すなわち、発行されるキー文字列毎に課金・請求処理を行う。課金・請求処理の方法として、大きく分けて、前払いする方法と後払いする方法とがある。

【００５８】前払いする場合について説明する。キー文字列を発行する時点（図２のステップＳ４または図６のステップＳ２４）で、請求書を発行する。キー文字列の有効期限が経過したら、または、使用料金が前払いした金額を超えたら、ログインできないようにする。図７に示したような方法で、契約更新の希望の有無について問い合わせ、ユーザが契約更新を希望したら、新しいキー文字列を発行し、請求書を発行する。このように、前払いの場合には、個々のキー文字列を発行する時点で請求書を発行する。

【００５９】次に、後払いする場合について説明する。有効期限をもって、その間の使用料金を加算していき、有効期限が経過したら、請求書を発行するとともに、そのキー文字列においてはログインできないようにして、ユーザが契約更新を希望したら、新しいキー文字列を発行する。新しいキー文字列においても、同様に、有効期限が経過したら請求書を発行する。

【００６０】以上のように、本実施の形態においては、ユーザＩＤ、パスワード、キー文字列の３つによりユーザの認証を行って、ユーザに使用許可を与えるようにしたので、安全性が高く、契約していない第三者により不正にアクセスされることが防止できるとともに、さらに、キー文字列毎に課金・請求処理を行うようにしたので、課金・請求管理が容易であるとともに、料金を支払わないユーザに対しては新しいキー文字列の発行を停止するようにすることもでき、料金の回収率を高くすることができる。

【００６１】実施の形態７．本実施の形態においては、インターネット上でアンケートに答えると、期間限定のサービスを受けられるキー文字列が提供されるという例について説明する。図１４は、本実施の形態の動作を説明するための図である。図１４の表示画面６０に示されるような所定のアンケートにユーザが答えたとする。サーバ２はアンケート結果を受信すると、入力項目のチェックを行い、問題がなければ、それをデータベースに登録するとともに、キー文字列を作成して、ユーザに送信する。ユーザ端末１には、図１４の表示画面６１に示されるように、送信されてきたキー文字列とともにその有効期限が表示される。ユーザが、図１４の表示画面６２に表示されているような「アンケートにお答えいただいた方には、期間限定の「特別価格」で購入できます。キー文字列を入力して送信ボタンを押して下さい。」というメッセージに従って、キー文字列を入力すると、所定の「特別価格」ページが画面に表示される。

【００６２】以上のように、本実施の形態においては、アンケートに答えた人に対してキー文字列を与え、ユーザＩＤ、パスワード、キー文字列の３つによりユーザの認証を行って、「特別価格」のページへのアクセスの許可を与えるようにしたので、安全性が高く、アンケートに答えていない第三者により不正にアクセスされることがなく、情報のセキュリティを守ることができる。また、アンケートに答えることにより、特別なサービスを受けることができるようにし、かつ、キー文字列を用いてサービス提供の期限管理を行うようにしたので、アンケートへの回答率の向上と期限管理処理との両面の効率化を図ることができる。

【００６３】実施の形態８．本実施の形態においては、特定のホームページ（もしくはホームページの特定のグループ会員）に登録したユーザにのみホームページ内の所定のページ（有資格領域）の内容が表示されるようにした例について説明する。図１５は、本実施の形態におけるホームページの一例を示したものであり、図において、７０は当該ホームページを表示している表示画面、７１は一般の人が参照できるフリー領域であり、７２はユーザ登録したユーザのみが参照できる有資格領域である。一般の人がアクセスすると、フリー領域７１のみが表示画面７０に表示される。一方、ユーザ登録したユーザがユーザＩＤ、パスワード、キー文字列を用いてアクセスすると、図１５のように、フリー領域７１及び有資格領域７２の両方が表示画面７０に表示される。

【００６４】なお、ユーザの登録動作については、上述の実施の形態１で説明した図２のフローチャートに示す処理に従い、ログインの動作は図４に、キー文字列更新の動作は図６に従うものとする。

【００６５】また、上述においては、登録してあるユーザがユーザＩＤ、パスワード、キー文字列の３つを用いてログインする例について示したが、その場合に限らず、ユーザＩＤとパスワードを用いてログインを行うようにしてもよく、その場合には、まず、図１６に示すように、フリー領域７１部分だけが表示され、その下に、「掲示板」というボタン７３が表示され、ユーザが「掲示板」ボタン７３にマウスポインタを当てると、「キー文字列を入力。」というメッセージが表示され、それに従って、ユーザがキー文字列を入力欄７４に入力して、送信ボタン７５を押すと、図１５の有資格領域７２に相当するページが表示画面７０に表示される。

【００６６】以上のように、本実施の形態においても、ユーザＩＤ、パスワード、キー文字列の３つによりユーザの認証を行って、ユーザに使用許可を与えるようにしたので、有資格領域を登録していない第三者により不正にアクセスされることがなく、情報のセキュリティを守ることができる。

【００６７】実施の形態９．本実施の形態においては、雑誌や本等の種々の文献の購読ができるホームページを想定して、その購読契約にキー文字列を用いる例につい

て説明する。図１７は当該ホームページにおけるユーザ登録及び購読契約を行うための表示画面を示したものである。上述の実施の形態１と同様の手順でユーザ情報を入力し、次に、文献名が記載されている任意のボタンをクリックして、購読契約を行いたい文献を指定した後に、送信ボタン８２を押すことにより、購読契約を行いたい文献情報がサーバ２に送信される。これを受けて、サーバ２は、キー文字列を発行し、ユーザに通知する。すなわち、上述の図２の処理と異なる点は、ステップＳ１において、ユーザ情報だけを入力せずに、購読契約を行いたい文献名も入力する点である。それ以外の処理は図２と同様である。このようにして、ユーザ登録及び購読契約を行ったユーザは、キー文字列の有効期限内において、図４の要領でログインすると、契約してある文献の内容を画面で参照またはダウンロードすることができる。なお、キー文字列の更新については、実施の形態１と同様に行う。

【００６８】なお、購読契約したい文献は１冊に限ることなく、複数冊を指定するようにしてもよい。その場合、各文献に対して、それぞれ、別のキー文字列を与えるようにし、課金・請求処理については、上述の実施の形態６で示したように、キー文字列ごとに各有効期間に対して課金・請求処理を行うようにする。

【００６９】図１８は、本実施の形態におけるデータベース３の一例を示したものである。各文献の契約に関するデータを図１８に示すように格納するようにすれば、各文献の契約有効期間や課金の管理を容易に行うことができる。図において、８５は各文献の契約に関するデータからなる契約管理データセット、８５ａは購読契約した文献名、８５ｂは契約をした日付、８５ｃは当該文献の購読有効期間、８５ｄは購読有効期間の延べ日数、８５ｅは購読料金、８５ｆは各文献に対して発行されたキー文字列である。延べ日数８５ｄは、１ケ月に満たない購読料金を日割り計算する場合のもので、１ケ月単位の契約の場合には“１Ｍ”，“２Ｍ”…というデータが格納される。なお、ここでの購読有効期間８５ｃはキー文字列の有効期限と同一のものである。従って、キー文字列の有効期間に、ユーザからのアクセスがあった場合には、サーバ２は、各文献に対して、契約管理データセット８５の内容を参照して、ユーザがアクセス可能か否かを検索するようにする。なお、本実施の形態においては、図１８のデータベース３内の３Ｘ部分については不要であるため、削除してもよい（３Ｘを用いる例について、後述の実施の形態１０においては説明する。）。

【００７０】以上のように、本実施の形態においても、ユーザＩＤ、パスワード、キー文字列の３つによりユーザの認証を行って、ユーザに契約文献へのアクセス許可を与えるようにしたので、購読契約をしていない第三者により不正にアクセスされることがなく、情報のセキュリティを守ることができる。

【００７１】実施の形態１０．上述の実施の形態においては、各文献ごとに異なるキー文字列を発行する例について述べたが、本実施の形態においては、ユーザの利便性を考えて、共通のキー文字列により、契約した文献がすべてアクセスできる例について説明する。

【００７２】例えば、最初に所定の文献について契約しておき、その後、別の日に他の所定の文献の契約をしたような場合には、２回目に契約したときに発行されたキー文字列により、最初に契約した分の文献についてもアクセスできるようにする。すなわち、最新の契約時に発行されたキー文字列を用いることにより、過去に契約した文献がすべて参照できるようにすれば、ユーザが複数のキー文字列を覚えておかなくてすむため、ユーザの負担を軽減することができる。

【００７３】なお、共通のキー文字列は、データベース３内の３Ｘ部分に格納する。このとき、各文献ごとの購読有効期間の管理や、課金・請求処理の管理をサーバ２が行うときのため、上述の実施の形態９で示したように、各文献ごとのキー文字列を発行してデータセット８５内のキー文字列８５ｆ内に格納するようにしてもよい。ユーザは共通のキー文字列を用いてアクセスを行い、サーバ２はユーザ認証には共通のキー文字列を用い、各文献ごとの購読有効期間の管理や、課金・請求処理の管理には個々のキー文字列８５ｆを用いる。

【００７４】なお、ここでの購読有効期間８５ｃは、共通のキー文字列の有効期限とは独立のものである。従って、この購読有効期間８５ｃを管理するための手段（図示省略）をサーバ２内に設けて、その手段により、購読有効期間を経過した文献についてはデータベース３からデータを削除するとともに、購読料金８５ｅのデータを基に請求書を作成してユーザに請求するようにする。このとき、個々の文献ごとに請求書を発行してもかまわないが、利便性を考慮すれば、請求書の発行は毎月１回とし、１つの請求書において複数の文献について請求するようにしてもよい。

【００７５】このように、購読有効期間を経過した文献についてはデータベース３から削除するようにしたので、共通のキー文字列の有効期間内に、ユーザからのアクセスがあった場合には、サーバ２はデータベース３の内容を参照して、ユーザがアクセス可能な文献を検索するようにする。

【００７６】このようにして、サーバ側においては個々のキー文字列を用いて契約文献の管理を行うようにすれば、発行日の異なる複数の雑誌を契約したような複雑な場合にも、ユーザにおいては１つの共通のキー文字列により、それらの文献の購読が可能になる。

【００７７】なお、上述の実施の形態１～１０においては、ユーザＩＤ、パスワード、キー文字列の３つの情報を組み合わせてユーザの認証を行う例について述べたが、この場合に限らず、本発明の目的は、ユーザが頻繁

にパスワードを変更しないことが多々あるため、サーバ側より強制的に定期的にユーザ認証のための情報を変更して安全性を向上させることであるため、ユーザＩＤとキー文字列だけを用いてユーザ認証を行うようにしてもよい。

【００７８】また、上述の実施の形態１～１０においては、ユーザ認証のための照合の順序を、ユーザＩＤ、パスワード、キー文字列の順で行う例について述べたが、この場合に限らず、ユーザＩＤ、キー文字列、パスワードの順でもよく、キー文字列、ユーザＩＤ、パスワードの順で行ってもよい。また、ユーザＩＤとキー文字列だけをユーザ認証に用いる場合には、キー文字列の照合を先に行うようにしてもよい。

【００７９】また、上述の実施の形態１～１０においては、ネットワークに接続されたサーバから構成されるユーザ認証システムについて説明したが、本発明はそれに限らず、パーソナルコンピュータやワークステーション等を含む種々の情報処理装置に適用することができる。

【００８０】

【発明の効果】この発明は、登録されるユーザを識別するための固有識別情報を入力するための入力手段と、ユーザを固有識別情報に基づいて管理するユーザ管理記憶手段と、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、ユーザ管理記憶手段に登録する認証システム指定特定情報登録手段と、登録された認証システム指定特定情報をユーザに通知する通知手段と、登録されている認証システム指定特定情報を変更もしくは無効にするように認証システム指定特定情報登録手段に所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力手段と、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合手段と、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可手段とを備えたユーザ認証システムであるので、認証システム側により所定の時間間隔で変更される認証システム指定特定情報を用いてユーザ認証を行うことにより、安全性を高め、第三者による不正アクセスを防止することができる。

【００８１】また、ユーザを特定するための情報の入力をユーザから受けて、当該情報をユーザ指定特定情報として、ユーザ管理記憶手段に登録するユーザ指定特定情報登録手段をさらに備え、照合手段が、上記照合に加えて、さらに、ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報をユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定するようにしたので、固有識別情報、認証システム側により所定の時間間隔で変更される認証システム指定特定情報、及び、ユーザ指定特定情報の３つの情報を組み合わせてユーザ認証を行うため、さらに安全性を高め、第三者による不正アクセスを防止することができる。

【００８２】また、通知手段が、認証システム指定特定情報を、ユーザからの固有識別情報の入力があった画面上に表示することによりユーザに通知するようにしたので、即座に通知することができる。

【００８３】また、通知手段が、認証システム指定特定情報を電子メールによりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【００８４】また、通知手段が、認証システム指定特定情報をＦＡＸによりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【００８５】また、通知手段が、認証システム指定特定情報を郵便物によりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【００８６】また、通知手段が、認証システム指定特定情報を暗号化してユーザに送信するようにしたので、第三者に特定情報が漏れる可能性を低減することができる。

【００８７】また、課金・請求処理を行うための課金処理手段をさらに備えているので、自動的に課金・請求処理が行え、利便性が向上する。

【００８８】また、認証システム指定特定情報の有効期間に対して課金・請求処理を行うための課金処理手段をさらに備え、認証システム指定特定情報毎に課金・請求処理を行うようにしたので、課金・請求処理のための管理が容易になり、また、料金を支払わないユーザに対しては次のキー文字列の発行を停止する等の制御も容易になる。

【００８９】また、この発明は、登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、ユーザを固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、データベースに登録する認証システム指定特定情報登録ステップと、登録された認証システム指定特定情報をユーザに通知する通知ステップと、登録

されている認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、指示に基づいて、データベースに登録されている認証システム指定特定情報を変更または無効にしてデータベースに再登録する認証システム指定特定情報再登録ステップと、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可ステップとを備えたユーザ認証方法であるので、認証システム側により所定の時間間隔で変更される認証システム指定特定情報を用いてユーザ認証を行うことにより、安全性を高め、第三者による不正アクセスを防止することができる。

【００９０】また、ユーザを特定するための情報の入力をユーザから受けて、当該情報をユーザ指定特定情報として、データベースに登録するユーザ指定特定情報登録手段をさらに備え、照合ステップにおいて、上記照合に加えて、さらに、ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報をユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定するようにしたので、固有識別情報、認証システム側により所定の時間間隔で変更される認証システム指定特定情報、及び、ユーザ指定特定情報の３つの情報を組み合わせてユーザ認証を行うため、さらに安全性を高め、第三者による不正アクセスを防止することができる。

【００９１】また、通知ステップにおいて、認証システム指定特定情報を、ユーザからの固有識別情報の入力があった画面上に表示することによりユーザに通知するようにしたので、即座に通知することができる。

【００９２】また、通知ステップにおいて、認証システム指定特定情報を電子メールによりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【００９３】また、通知ステップにおいて、認証システム指定特定情報をＦＡＸによりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【００９４】また、通知ステップにおいて、認証システム指定特定情報を所定の郵便物によりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【００９５】また、通知ステップにおいて、認証システム指定特定情報を暗号化してユーザに送信するようにしたので、第三者に特定情報が漏れる可能性を低減することができる。

【００９６】また、課金・請求処理を行うための課金処理ステップをさらに備えているので、自動的に課金・請求処理が行え、利便性が向上する。

【００９７】また、認証システム指定特定情報の有効期間に対して課金・請求処理を行うための課金処理ステップをさらに備え、認証システム指定特定情報毎に課金・請求処理を行うようにしたので、課金・請求処理のための管理が容易になり、また、料金を支払わないユーザに対しては次のキー文字列の発行を停止する等の制御も容易になる。

【００９８】また、この発明は、ユーザ認証を行うためのプログラムを記録した記録媒体であって、登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、ユーザを固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、データベースに登録する認証システム指定特定情報登録ステップと、登録された認証システム指定特定情報をユーザに通知する通知ステップと、登録されている認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、指示に基づいて、データベースに登録されている認証システム指定特定情報を変更または無効にしてデータベースに再登録する認証システム指定特定情報再登録ステップと、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可ステップとを備えたプログラムを記録した記録媒体であるので、このプログラムを用いて、認証システム側により所定の時間間隔で変更される認証システム指定特定情報を用いてユーザ認証を行うことにより、安全性を高め、第三者による不正アクセスを防止することができるとともに、プログラム

25

が記録媒体に記録されているので、種々のシステムに容易に当該プログラムを搭載することができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１におけるユーザ認証システムの構成を示したブロック図である。

【図２】　本発明の実施の形態１におけるユーザ認証システムにおいてユーザ登録を行う場合の処理の流れを示したフローチャートである。

【図３】　図２の動作を説明するための説明図である

【図４】　本発明の実施の形態１におけるユーザ認証システムにおいてキー文字列の有効期限内にログインを行う場合の処理の流れを示したフローチャートである。

【図５】　図４の動作を説明するための説明図である

【図６】　本発明の実施の形態１におけるユーザ認証システムにおいてキー文字列の更新を行う場合の処理の流れを示したフローチャートである。

【図７】　図６の動作を説明するための説明図である

【図８】　本発明の実施の形態２におけるユーザ認証システムにおいてユーザ登録を行う場合の処理の流れを説明するための説明図である。

【図９】　本発明の実施の形態２におけるユーザ認証システムにおいてキー文字列の更新を行う場合の処理の流れを説明するための説明図である。

【図１０】　本発明の実施の形態４における課金処理手段を加えたユーザ認証システムにおいてユーザ登録を行う場合の処理の流れを説明するための説明図である。

【図１１】　本発明の実施の形態５におけるユーザ認証システムにおいてユーザ登録を行う場合の処理の流れを説明するための説明図である。

【図１２】　本発明の実施の形態５におけるユーザ認証システムにおいて１ケ月目のログインを行う場合の処理の流れを説明するための説明図である。

26

【図１３】　本発明の実施の形態５におけるユーザ認証システムにおいてキー文字列の更新を行う場合の処理の流れを説明するための説明図である。

【図１４】　本発明の実施の形態６におけるユーザ認証システムにおいてアンケートへの回答及び特別サービスへのアクセスを行う場合の処理の流れを説明するための説明図である。

【図１５】　本発明の実施の形態７におけるユーザ認証システムによるホームページの一例を表示した表示画面を示す図である。

【図１６】　本発明の実施の形態７におけるユーザ認証システムによるホームページの他の例を表示した表示画面を示す図である。

【図１７】　本発明の実施の形態８におけるユーザ認証システムによるホームページの一例を表示した表示画面を示す図である。

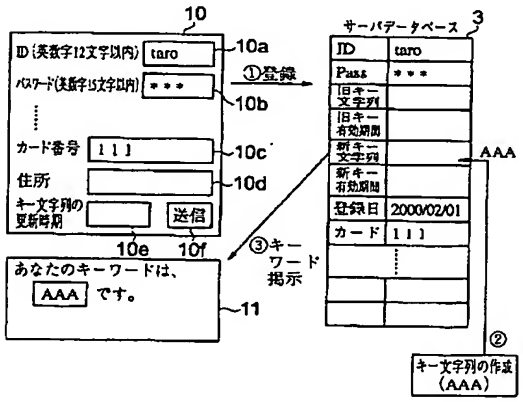
【図１８】　本発明の実施の形態８におけるユーザ認証システムにおける購読契約を行った文献を管理するためのデータが追加されたデータベースの一例を示した図である。

【図１９】　従来のユーザ認証システムが設けられたネットワークシステム全体を示した概略構成図である。

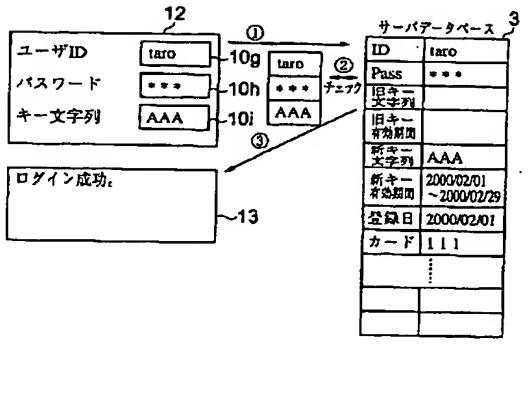
【符号の説明】

１　ユーザ端末、２　サーバ、２ａ　ユーザインターフェース手段、２ｂ　ユーザ指定特定情報登録手段、２ｃ　認証システム指定特定情報登録手段、２ｄ通知手段、２ｅ　変更／無効指示出力手段、２ｆ　第一の照合手段、２ｇ　第二の照合手段、２ｈ　第三の照合手段、２ｉ　制御手段、２ｊ　メインプログラム格納手段、２ｋ　データベースインターフェース手段、３　データベース、４メールサーバ、５　課金処理手段。

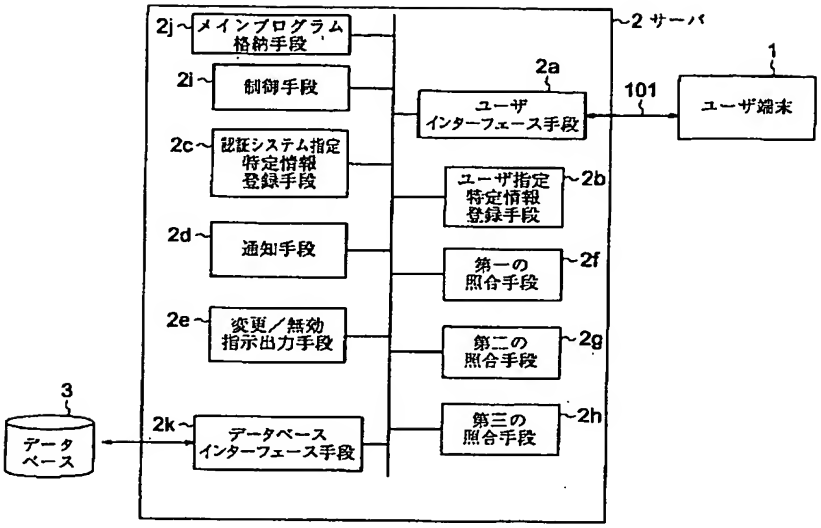
【図３】



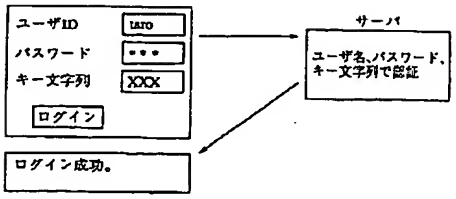
【図５】



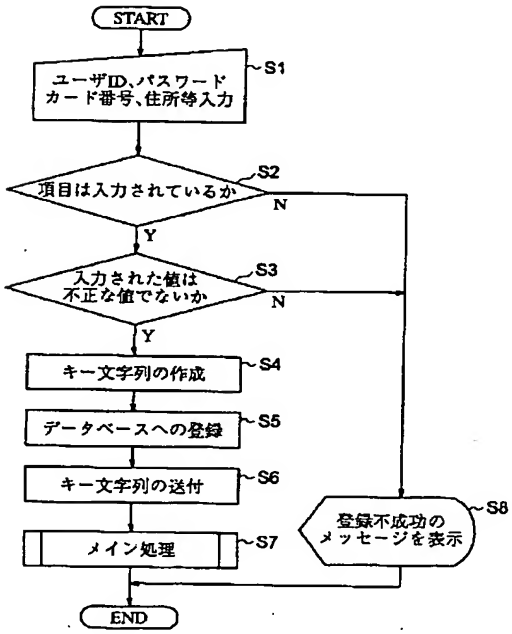
【図１】


2 サーバ
2j メインプログラム格納手段
2i 制御手段
2c 認証システム指定特定情報登録手段
2d 通知手段
2e 変更／無効指示出力手段
2k データベースインターフェース手段
2a ユーザインターフェース手段
2b ユーザ指定特定情報登録手段
2f 第一の照合手段
2g 第二の照合手段
2h 第三の照合手段
101
1 ユーザ端末
3
データベース

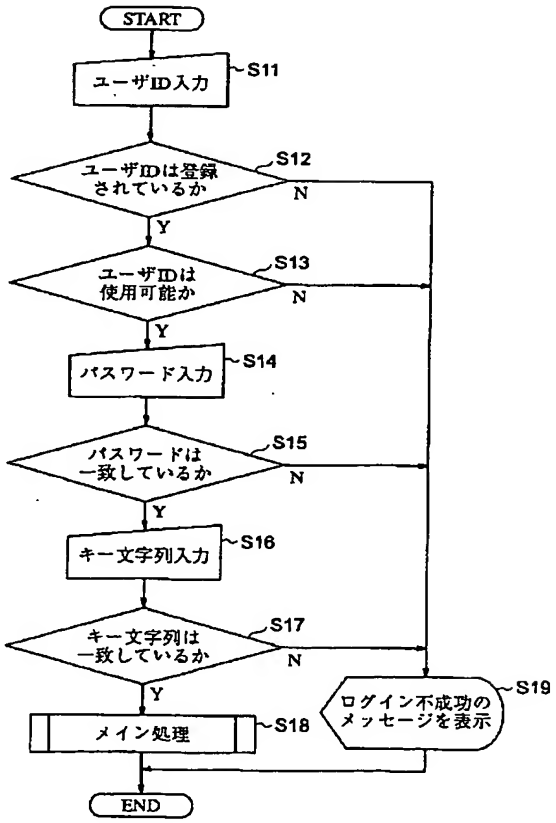
【図１２】


ユーザID
taro
パスワード
***
キー文字列
XXX
ログイン
サーバ
ユーザ名、パスワード、キー文字列で認証
ログイン成功。

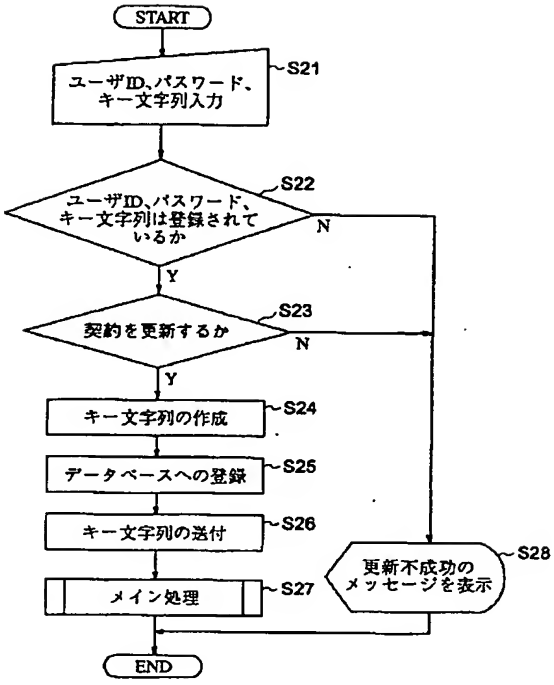
【図２】


START
ユーザID、パスワード カード番号、住所等入力
S1
項目は入力されているか
S2
N
Y
入力された値は不正な値でないか
S3
N
Y
キー文字列の作成
S4
データベースへの登録
S5
キー文字列の送付
S6
メイン処理
S7
登録不成功のメッセージを表示
S8
END

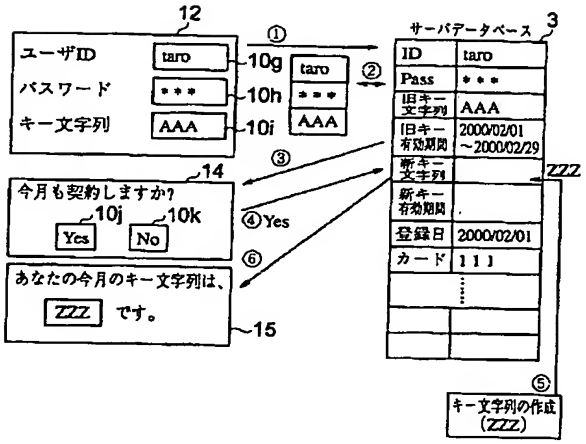
【図４】


START
ユーザID入力
S11
ユーザIDは登録されているか
S12
N
Y
ユーザIDは使用可能か
S13
N
Y
パスワード入力
S14
パスワードは一致しているか
S15
N
Y
キー文字列入力
S16
キー文字列は一致しているか
S17
N
Y
メイン処理
S18
ログイン不成功のメッセージを表示
S19
END

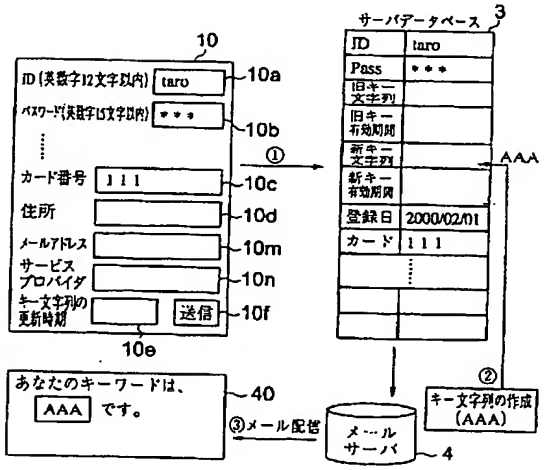
【図６】


START
ユーザID、パスワード、キー文字列入力
S21
ユーザID、パスワード、キー文字列は登録されているか
S22
N
Y
契約を更新するか
S23
N
Y
キー文字列の作成
S24
データベースへの登録
S25
キー文字列の送付
S26
メイン処理
S27
更新不成功のメッセージを表示
S28
END

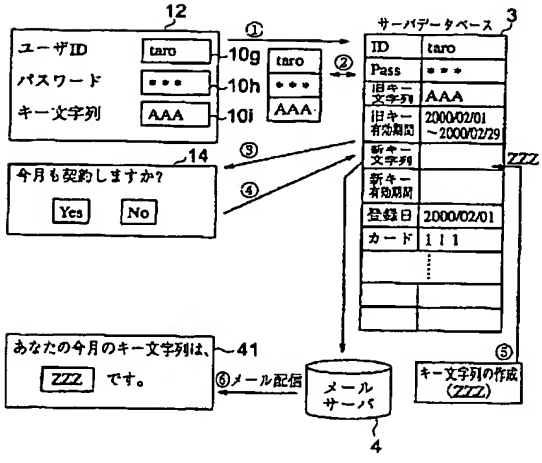
【図７】


12
ユーザID
taro
10g
パスワード
***
10h
キー文字列
AAA
10i
①
②
③
14
今月も契約しますか?
10j
Yes
10k
No
④Yes
⑥
あなたの今月のキー文字列は、
ZZZ
です。
15
サーバデータベース
3
ID taro
Pass ***
旧キー文字列 AAA
旧キー有効期間 2000/02/01 ～2000/02/29
新キー文字列 ZZZ
新キー有効期間
登録日 2000/02/01
カード 111
⑤
キー文字列の作成 (ZZZ)

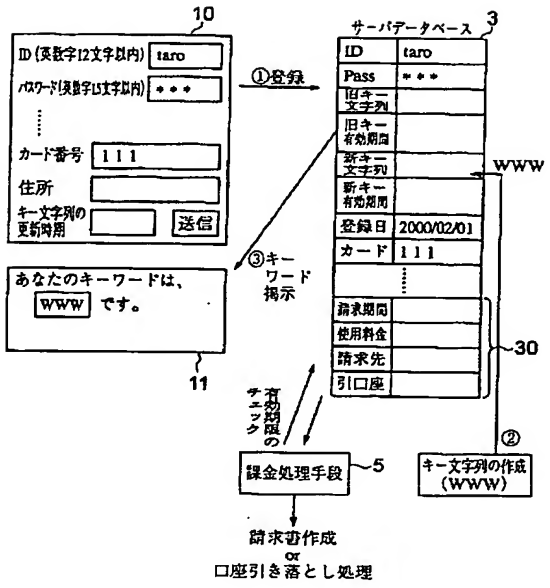
【図８】


10
ID (英数字12文字以内) taro
10a
パスワード (英数字16文字以内) ***
10b
カード番号 111
10c
住所
10d
メールアドレス
10m
サービスプロバイダ
10n
キー文字列の更新時期
送信
10f
10e
①
サーバデータベース
3
ID taro
Pass ***
旧キー文字列
旧キー有効期間
新キー文字列 AAA
新キー有効期間
登録日 2000/02/01
カード 111
②
キー文字列の作成 (AAA)
あなたのキーワードは、
AAA
です。
40
③メール配信
メールサーバ
4

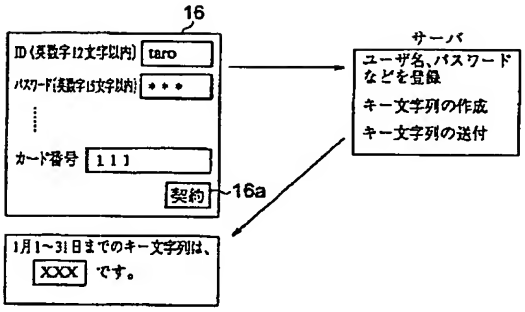
【図９】


12
ユーザID
taro
10g
パスワード
***
10h
キー文字列
AAA
10i
①
②
③
14
今月も契約しますか?
Yes
No
④
サーバデータベース
3
ID taro
Pass ***
旧キー文字列 AAA
旧キー有効期間 2000/02/01 ～2000/02/29
新キー文字列 ZZZ
新キー有効期間
登録日 2000/02/01
カード 111
⑤
キー文字列の作成 (ZZZ)
あなたの今月のキー文字列は、
ZZZ
です。
41
⑥メール配信
メールサーバ
4

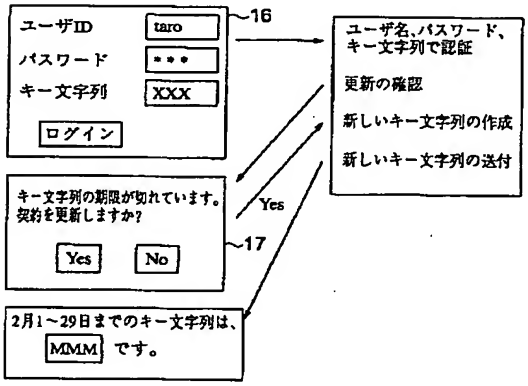
【図１０】



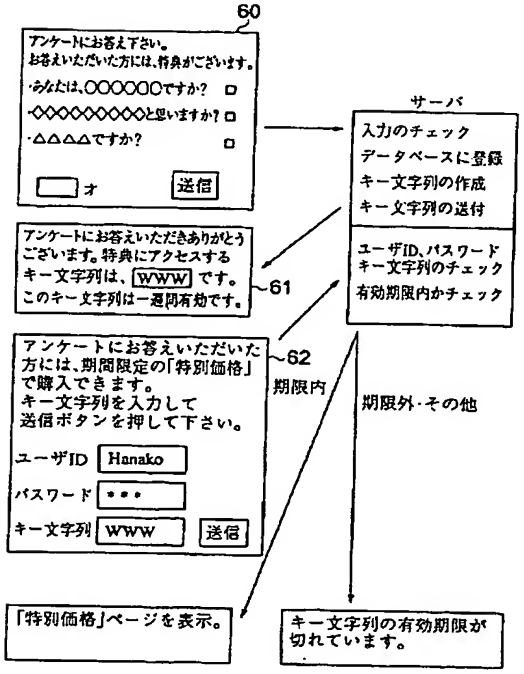
【図１１】



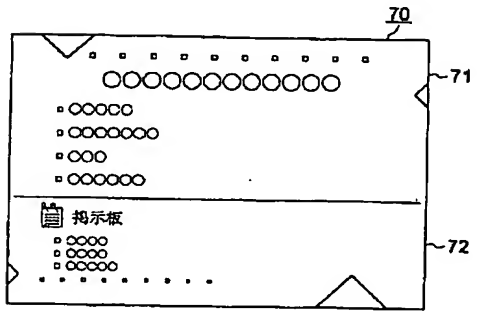
【図１３】



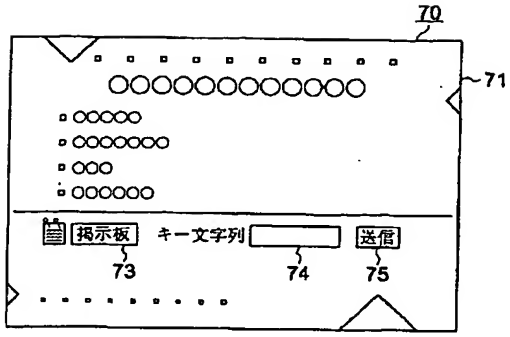
【図１４】



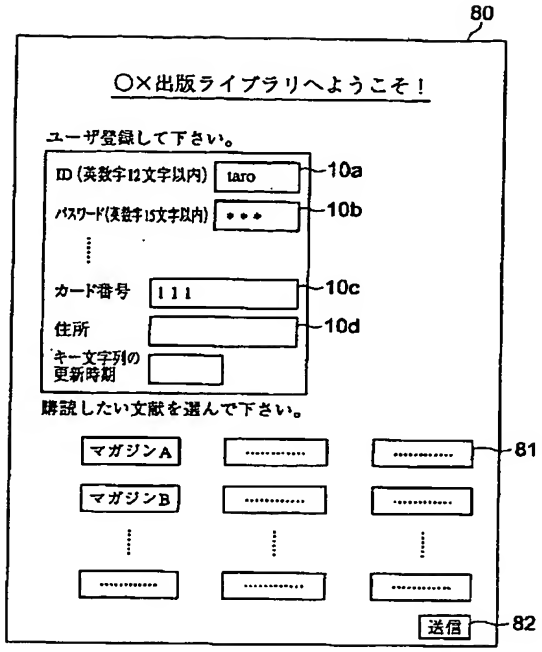
【図１５】



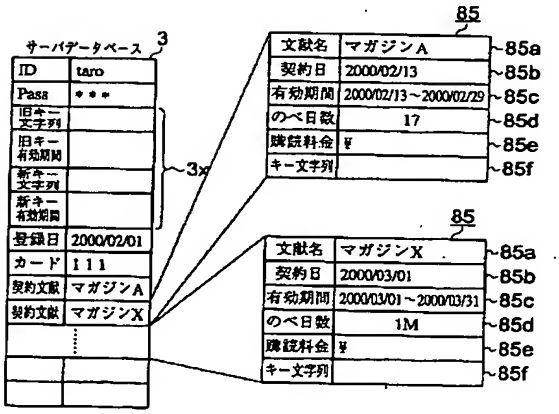
【図１６】



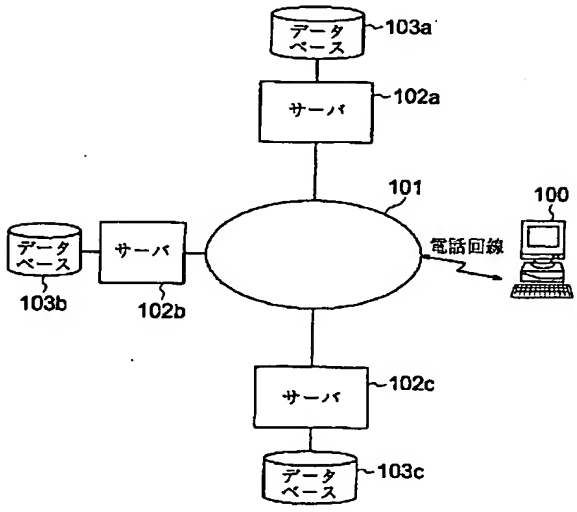
【図１７】



【図１８】



【図１９】



101：ネットワーク